IN THE CLAIMS:

Claims 1 to 51 have been cancelled in prior amendments.

Claims 52 to 60 are cancelled in this amendment

Claims 61 to 66 have been cancelled in the prior amendment .

Claim 67 is withdrawn due to restriction requirements

Claims 68 to 70 are cancelled in the prior amendment.

Claim 71 is cancelled in this amendment.

72 to 76 cancelled in the prior amendments.

77. (previously and currently amended) A method of protecting bankcard data and securely selecting any one of a plurality [[~~at least two~~]] of bankcards of a customer at a merchant point of sale for a payment to a merchant comprising the steps of:

a. entering of a customer identifier, without customer identity of name and bankcard number, and a bankcard specific personal identification number (CPIN) in the point of sale (POS) interface;

b. sending the identifier and the CPIN, by the POS, to a merchant gateway [[~~card processor~~]];

c. interfacing by the merchant gateway [[~~card processor~~]] with a third party payment system, wherein the customer having a plurality of [[~~at least two~~]] pre-stored customer bankcard data, each bankcard identified with the CPIN;

d. sending by the gateway to the payment system the customer identifier and the CPIN [[~~returning to the card processor the bankcard data corresponding to the customer identifier and the CPIN from the payment system~~]].

78. (currently amended) The [[claim]] method as in claim 77, having further step of:

a. identifying a particular bankcard of the customer and verifying the customer by the CPIN in the payment system;[[.]]

b. returning to the merchant gateway the bankcard data corresponding to the customer identifier and the CPIN from the payment system.

79. (currently amended) The [[Claim]] method as in claim [[77]] 78, having further step of:

processing the payment transaction with the bankcard data by the merchant gateway by submitting a prior art payment transaction record to a prior art card authorization network [[~~card processor~~]].

80. (currently amended) The [[Claim]] method as in claim [[78]] 77, having further steps of:

a. having access to the payment system by the customer;

b. entering the bankcard data and self-selecting a CPIN for each bankcard of the customer.

Claims 81 to 85 are cancelled in the prior amendments

Claims 86 to 93 are withdrawn due to restriction requirements.

94. (newly added) A payment card system that protects private data of customer in customer to merchant payment transactions, comprising:

a. a payment card with a substrate pre-encoded with a customer identifier that is without a name and bank data, the identifier maps to the payment system;

b. the substrate preprinted with an alias name selected by the customer.

95. (newly added) The payment card system as in claim 94, comprising:
the encoding medium is a magnetic strip.

96. (newly added) The payment card system as in claim 94, comprising:
the customer-identifier is self-created by the customer.

97. (newly added) The payment card system as in claim 94, further comprising:

a. an adapted prior art merchant gateway, the customer identifier from the payment card used for a payment transaction at a merchant POS, along with entry of a CPIN by the customer, routed to the adapted prior art merchant gateway, the adaptation in the prior art gateway routes the customer identifier and the CPIN to the payment system;

b. the payment system maps the customer identifier and the CPIN to retrieve pre-stored bankcard data and returns to the adapted prior art gateway, for submission of a prior art payment transaction to prior art card authorization network, thereby the payment card of this invention does not transfer customer identity data to the merchant POS.

98. (newly added) The payment card system as in claim 94, further comprising:

the customer identifier as pre-encoded on the substrate is pre-encrypted, and embeds a reference to an encryption algorithm; the payment system decrypts the customer identifier using the referenced algorithm, and then uses the customer identifier to retrieve customer bankcard data in the payment system.

99. (newly added) A method of conducting a payment transaction that protects the privacy of customer identity and bankcard data, comprising the steps of:

delivering to a customer, a payment card with a substrate preprinted with an alias name selected by the customer and pre-encoded with a customer identifier that is without a name and bankcard data, the identifier maps to a payment system.

100. (newly added) The method as in claim 99, further comprising the steps of:

a. using the payment card for a payment transaction at a merchant POS and entering a CPIN by the customer;

b. the POS routing the payment transaction record to an adapted prior art merchant gateway;

c. identifying the use of the payment card at POS, by the adapted gateway, and routing the customer identifier and CPIN of the transaction to the payment system.

101. (newly added) The method as in claim 100, further comprising the steps of:

connecting wirelessly by the merchant POS to the payment system for routing customer identifier and the CPIN, thereby bypassing the gateway as in steps (b) and (c) of the preceding claim.

102. (newly added) The method as in claim 101, further comprising the steps of:

using the customer identifier and the CPIN, retrieving pre-stored bankcard data in the payment system, and returning to the prior art gateway, enabling the gateway to form a prior art payment approval request for submitting the prior art payment approval request to a prior art card authorization network, wherein the payment card of this invention does not transfer customer identity data to the merchant POS

103. (newly added) The method as in claim 102, further comprising the steps of:

a. encrypting the customer identifier that is encoded on the substrate by the payment system;

b. decrypting the customer identifier by the payment system before retrieving the customer bankcard data.

104. (newly added) A payment security system that provides identity security in use of bankcards, comprising:

a. a customer identifier that is without customer name and bankcard data;

b. the customer identifier anchors a plurality of bankcard data of the customer, each identified with a card specific personal identification number (CPIN) in the payment security system;

c. the customer identifier encrypted with an aliasing algorithm from a list of such algorithms in a database maintained by the security system and the encrypted identifier and the algorithm reference number are encoded on a payment card encoding mechanism, wherein the payment card and the CPIN is used by the customer at a merchant point of sale terminal (POS) for conducting a payment transaction.

105. (newly added) The payment security system as in claim 104, further comprising:

on swiping of the payment card and entry of the CPIN, the system receives from the merchant POS, the encrypted customer identifier and the CPIN, decrypts the customer identifier, selects the CPIN specific bankcard data of the customer for processing a payment transaction with a prior art card processing network, wherein, the security system does not identity the customer and customer bankcard data to merchant systems.